FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER: 0745/65813/NHZ

U.S APPLICATION NO (If known, see 37 CFR 1 5): 09/936420

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE00/00752	13 March 2000	12 March 1999

TITLE OF INVENTION: METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS OF COMMUNICATIONS NETWORKS

APPLICANT(S) FOR DO/EO/US: Peter BRUNE and Andreas SASSE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [X] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [X] is attached hereto (required only if not communicated by the International Bureau).
   b. [ ] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [X] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [X] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [X] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [X] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [X] Other items or information: A copy of the International Application as published, including International Search Report and translations thereof, Express Mail Certificate of Mailing dated 12 September 2001, bearing label No. EK146 828 343US.

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/936420	PCT/DE00/00752	0745/65813/NHZ

21. [X] The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$1,000.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$0	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	8 - 20 =	0	x **$18.00**	$0	
Independent claims	0 - 3 =	0	x **$80.00**	$0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)	0		+ **$270.00**	$0	
TOTAL OF ABOVE CALCULATIONS =				$1,000.00	
[ ] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.			+	$	
SUBTOTAL =				$1,000.00	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$	
TOTAL NATIONAL FEE =				$	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
TOTAL FEES ENCLOSED =				$1,000.00	
				Amount to be refunded:	$
				charged:	$

a. [X] A check in the amount of $ 1,000.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 03-3125. A duplicate copy of this sheet is enclosed.

d. [ ] Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Norman H. Zivin
COOPER & DUNHAM LLP
1185 Avenue of the Americas
New York, New York 10036

SIGNATURE

Norman H. Zivin
NAME

25,385
REGISTRATION NUMBER

Dkt. 65813

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Peter BRUNE and Andreas SASSE
Serial No.	:	Not Yet Known
Filed	:	Herewith
For	:	METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS IN COMMUNICATIONS NETWORKS

Assistant Commissioner of Patents
BOX PCT
Washington, D.C. 20231

Sir:

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: **EK146 828 343US**

Date of Deposit: **September 12, 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231

Jamel Khabb
Printed Name:
Jamel Khabb

Respectfully submitted,

Date: September 12, 2001

Norman H. Zivin
Reg. No. 25,385
Attorney for Applicant
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400

Dkt. 65813

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Peter BRUNE and Andreas SASSE
Serial No.	:	Not Yet Known
Filed	:	Herewith
For	:	METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS IN COMMUNICATIONS NETWORKS

Assistant Commissioner of Patents
BOX PCT
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Please delete the claims, and substitute new claims 1 through 8, as follows:

-- 1. A method for distributing keys to subscribers in digital mobile radio networks, with the keys being generated, and possibly being stored if required, in a security device provided at the mobile radio network end and, on request by a subscriber, at least one key being requested from the security device and being transmitted via the mobile radio network to a mobile station or a terminal of the subscriber, characterized in that the transmitted key is allocated to that subscriber, and is stored in the terminal and/or in a subscriber identity module SIM in the mobile station.

2. The method as claimed in claim 1, characterized in that an SAT application is set up in the subscriber identity module SIM, in the mobile station, and carries out additional end-to-end encryption of the key transmitted between the mobile station and the security device.

3. The method as claimed in claim 2, characterized in that, in order to use the SAT application, the subscriber must identify himself to the subscriber identity module SIM by entering a PIN.

4. The method as claimed in claim 1, characterized in that the transmitted key is stored in a protected memory area in the subscriber identity module SIM.

5. The method as claimed in claim 1, characterized in that the key is transmitted via a traffic channel in the mobile radio network.

6. The method as claimed in claim 1, characterized in that the key is transmitted in the form of a short message SM via a signaling channel in the mobile radio network.

7. The method as claimed in claim 1, characterized in that, when the key is requested, the subscriber's authorization is checked by evaluating a mobile subscriber telephone number MSISDN for the subscriber.

8. The method as claimed in claim 1, characterized in that the security device sends the key which is transmitted to the subscriber to one or more added value service nodes. --

REMARKS

The claims pending in the PCT application have been amended to eliminate multiple dependent claims. New claims 1 through 8 are presented for examination.

An early and favorable examination on the merits is earnestly solicited.

Respectfully submitted,

Dated: September 12, 2001 By: _____

Norman H. Zivin
Reg. No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400
Attorney for Applicant

LAWYERS' AND MERCHANTS' TRANSLATION BUREAU, INC.
Legal, Financial, Scientific, Technical and Patent Translations
11 BROADWAY
NEW YORK, NY 10004

Certificate of Accuracy

TRANSLATION
From **German into English**

STATE OF NEW YORK }
COUNTY OF NEW YORK } s.s.:

On this day personally appeared before me who, after being duly sworn, deposes and states: Elisabeth A. Lucas

That he is a translator of the **German** and English languages by profession and as such connected with the **LAWYERS' & MERCHANTS' TRANSLATION BUREAU;**

That he is thoroughly conversant with these languages;

That he has carefully made the attached translation from the original document written in the **German** language; and

That the attached translation is a true and correct English version of such original, to the best of his knowledge and belief.

SUBSCRIBED AND SWORN TO BEFORE ME THIS

Susan Tapley

Susan Tapley
Notary Public, State of New York
No. 01TA4999804
Qualified in Queens County
Certificate filed in New York County and Kings County
Commission Expires July 27, 2002

Method for distributing keys to subscribers in communications networks

The invention relates to a method for distributing keys to subscribers in communications networks, in particular digital mobile radio networks, as claimed in the pre-characterizing clause of the independent patent claim. These keys allow the user of a terminal to, for example, authenticate himself to an added value service node in the communications network.

At the moment, a subscriber to telecommunications services authenticates himself for access to added value service nodes, such as a mobile box, by entering a password and user name. In this case, the mobile subscriber telephone number (MSISDN) is generally transmitted as the user name by signaling in GSM mobile radio networks, without there being any explicit input by the user.

The allocation and use of the password (which in this context has the same meaning as a key) is a critical process since misuse can cause considerable damage if it is undesirably disclosed or the user is deliberately spied on. New passwords are thus frequently sent by registered letter which, organizationally and technically, involves considerable effort and, at the same time, a time delay before the user receives a password.

If, furthermore, the added value service node is accessed via networks that are not secure, such as the Internet, there is a risk of the user name and password being monitored without authorization, and being misused.

DE-A-197 18 103 discloses a method for authentication in data transmission systems, in which, on request by a subscriber, a key is generated in the form of a transaction number (TAN) by an authentication computer provided in the data transmission system, or is selected from a file. The key is transmitted from the authentication computer to the subscriber, where it can be used directly by the subscriber for authentication to the authentication computer. The distribution of a number of keys which can be used by the subscriber as required is not disclosed in this document.

The object of the invention is to specify a method using which keys can be distributed automatically to communications network subscribers using secure means.

According to the invention, this object is achieved by the characterizing features of the independent patent claim.

The essence of the invention is that the keys are generated, and may be stored if required, in a security device provided at the mobile radio network end, and in that on request by a subscriber, at least one key is requested from the security device, is allocated to the subscriber, and is transmitted via the mobile radio network to the

subscriber's mobile station or terminal, with the transmitted key being allocated to that subscriber and being stored in the terminal and/or a subscriber identity module (SIM) in the mobile station for further use.

The described method is particularly suitable for distributing keys automatically to mobile terminals by secure means in a GSM or UMTS network, and for storing them on the subscriber's (U)SIM. A terminal user can use these keys to authenticate himself to an added value service node. The (U)SIM provides a protected-access medium in order to check passwords or keys, to store them and, when required, to use them for authentication, from a mobile radio network.

Electronic and secure distribution and the automation resulting from this result firstly in a considerable reduction in effort and gain in time compared to conventional key distribution methods, which are generally based on receipted written communications. Secondly, the automated sequence, and hence the exclusion of human activities from key generation and distribution lead to an improvement in security.

Simple distribution furthermore allows more frequent distribution of keys with little effort. This also allows the use of simple authentication methods for access to added value service nodes in a telecommunications network, in which, for example, a specific key is used only once.

The authorized (U)SIM user can use the capability of transferring the key to other terminals and/or of accessing added value service nodes using the mobile terminal or other terminals via Internet, PSTN or ISDN. The authentication method between the terminal and the added value service node and the transfer of a key from the mobile terminal to another terminal can be achieved using existing algorithms, and is not the subject matter of the invention.

A first embodiment variant of the invention provides for the user to use a short message (SMS) to call for a new key when required. To do this, he sends a short message with specific contents to a destination address, which is defined in advance by the network operator and is associated with a security device. In response, he receives a password in plain

text back from this address. The user can now use this password to authenticate himself to an added value service node.

A second embodiment variant of the invention, which has a higher security level, provides for all the communications processes between the mobile station and the security device to be encrypted using an end-to-end encryption method by using a program on the (U)SIM (card application), which acts as the client to communicate with the mobile radio network. The program advantageously allows the user to be offered a menu-controlled interface on the mobile terminal, by means of which keys can be called up and managed.

In order to request a key, the user, for example, selects an appropriate menu item on his terminal. The mobile radio network responds with an encrypted message, which is sent directly to the card application. The card application stores the key in a protected memory area in the (U)SIM.

To authenticate himself to an added value service node, the user selects an appropriate menu item, for example, after entering a PIN. Depending on the authentication algorithm:

- either the key is displayed in plain text and can be reused by the user;
- the key is transmitted directly to the added value service node; or

- the key is transferred to another terminal, where it can be reused.

Advantageous refinements and developments of the invention are specified in the dependent patent claims.

The invention will be described in more detail in the following text using an example and with reference to a drawing figure. Further features and advantages of the invention are disclosed in the example, the drawing and its description.

Figure 1 shows an illustration of the systems involved in carrying out the method.

The mobile station 3, which comprises a terminal 4, has, in a known manner, the (U)SIM 5, in which the keys for user authentication are stored. The security device comprises a security server 9, which produces the keys using an algorithm selected by the operator, stores them in a data bank 10, and distributes the keys on request 1 from a subscriber to the (U)SIM 5 and to the added value service nodes 11 which can be used by that subscriber.

The short message service center 8 in the mobile radio network 7 transmits the keys in the form of short messages (SM) 2 between the security server 9 and the mobile station 3. This is shown only by way of example. GPRS nodes, for example, can also be used as transmission devices.

On the basis of a first security level used in the method according to the invention, the subscriber requests a key via his mobile station 3 by means of a short message 1.

The security server 9 evaluates the request by checking the transmission address (MSISDN) of the subscriber for authorization, and sends the key or keys in a short message 2 to the mobile station 3, where it or they is or are stored on the (U)SIM 5. Furthermore, the security server 9 sends the key to one or more added value service nodes 11. This completes the key distribution process. Depending on the chosen terminal 4 and access means (mobile radio, ISDN, Internet, etc.), the user can now authenticate himself to the added value service node 11.

With this low, first security level, the key distribution security is based on the protection against monitoring in the GSM/UMTS network and user identification by means of the MSISDN. Once they have been stored on the (U)SIM, the keys are protected by means of the standard PIN.

In the second, higher security level, the SIM Application Toolkit (SAT) in accordance with GSM 11.14 can be used. This is done by entering an SAT application in the (U)SIM 5, which communicates using this client-server configuration with the security server 9 via the GSM or UMTS network 7.

The user uses the menu on his terminal 4 to request keys via the SAT application. To do this, he must identify himself to the (U)SIM 5 using a second PIN which, for example, he enters via the keypad on the terminal 4. The SAT application then sends an encrypted request 1 to the security server 9, which processes the request. The security server 9

checks that the encrypted request is real, on the basis of the encryption and the address from which it was sent (MSISDN).

If the check result is positive, the security server 9 produces the key or keys for the user and sends it or them back to the SAT application in the (U)SIM 5. The SAT application receives the keys and stores them in a specially protected area in the (U)SIM 5. Furthermore, the security server 9 sends the key to one or more added value service nodes 11.

The keys can in turn be accessed under menu control by entering a PIN via the card application, which indicates an unused key on the display on the terminal 4 and, if desired, stores it in an unprotected SIM card memory area. From there, this key can be read to a PC/laptop by means of standard access software, for example by means of a smartcard reader or infrared interface in the GSM/UMTS terminal.

Alternatively, and depending on the security requirement, the key can also remain concealed from the user and can be transmitted in confidential form between the (U)SIM 5 and the added value service nodes 11, and/or from the (U)SIM 5 to the laptop/PC for later use.

One particular characteristic feature of the second security level is additional encryption of the short messages 1, 2 exchanged between the security server 9 (server SW) and the software in the (U)SIM (client SW). This provides end-to-end security between the server SW and the client SW. In this

case, the user preferably has no knowledge of the keys required for this purpose. Standard methods, such as triple DES or RSA, can be used as encryption algorithms between the client and server.

The keys required for additional encryption are entered once during personalization of the (U)SIM and are loaded in the security server.

Drawing legend

1 Signal flow: request key

2 Signal flow: load key

3 Mobile station

4 Terminal

5 (U)SIM

6 Air interface

7 Mobile radio network

8 Short message service center

9 Security device (server)

10 Data bank

11 Added value service node

Patent Claims

1. A method for distributing keys to subscribers in digital mobile radio networks (7), with the keys being generated, and possibly being stored if required, in a security device (9) provided at the mobile radio network end and, on request by a subscriber, at least one key being requested from the security device (9) and being transmitted via the mobile radio network (7) to a mobile station (3) or a terminal (4) of the subscriber,

characterized

in that the transmitted key is allocated to that subscriber, and is stored in the terminal (4) and/or in a subscriber identity module SIM (5) in the mobile station (3).

2. The method as claimed in claim 1, characterized

in that an SAT application is set up in the subscriber identity module SIM (5) in the mobile station (3), and carries out additional end-to-end encryption of the key transmitted between the mobile station (3) and the security device (9).

3. The method as claimed in claim 2, characterized

in that, in order to use the SAT application, the subscriber must identify himself to the subscriber identity module SIM (5) by entering a PIN.

4. The method as claimed in one of claims 1 to 3, characterized

in that the transmitted key is stored in a protected memory area in the subscriber identity module SIM (5).

5. The method as claimed in one of claims 1 to 4, characterized
in that the key is transmitted via a traffic channel in the mobile radio network (7).

6. The method as claimed in one of claims 1 to 4, characterized
in that the key is transmitted in the form of a short message SM via a signaling channel in the mobile radio network (7).

7. The method as claimed in one of claims 1 to 6, characterized
in that, when the key is requested, the subscriber's authorization is checked by evaluating a mobile subscriber telephone number MSISDN for the subscriber.

8. The method as claimed in one of claims 1 to 7, characterized
in that the security device (9) sends the key which is transmitted to the subscriber to one or more added value service nodes (11).

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States Application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37. Code of Federal Regulations. Sections 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	*Filing Date*	*Status*

(7) *And I hereby appoint* ***Norman H. Zivin (Reg. No. 25,385); John P. White (Reg. No. 28,678); Ivan S. Kavrukov (Reg. No. 25,161); Christopher C. Dunham (Reg. No. 22,031); Robert D. Katz (Reg. No. 30,141); Peter J. Phillips (Reg. No. 29,691); and Wendy E. Miller (Reg. No. 35,615)*** *and each of them, all c/o Cooper & Dunham LLP of 1185 Avenue of the Americas, New York, New York 10036 (Tel. 212 278-0400), my attorneys, each with full power of substitution and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent, to transact all business in the Patent and Trademark Office connected herewith and to file any International Applications which are based thereon under the provisions of the Patent Cooperation Treaty.*

Please address all communications, and direct all telephone calls, regarding this application to:

Norman H. Zivin *Reg. No.* ***25,385***
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
Tel. (212) 278-0400

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first joint inventor Peter BRUNE

Inventor's signature Peter Brune

Citizenship Germany *Date of signature* 21/09/01

Residence Noldestrasse 56
D-53340 Meckenheim, GERMANY DEX

Post Office Address SAME AS RESIDENCE

Dkt. 65813

#4

DECLARATION AND POWER OF ATTORNEY

As a below-named inventors, We hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS OF COMMUNICATIONS NETWORKS
(Title of Invention)

the specification of which:
(check one)

___ *is attached hereto.*

___ *was filed on* September 12, 2001

Application Serial No. 09/936,420

and was amended _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information of which I am aware which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			*Priority Claimed*	
Number	*Country*	*Filing Date*	*Yes*	*No*
199 11 221.5	*GERMANY*	*March 12, 1999*	*Yes*	___
PCT/DE00/00752	*PCT*	*March 13, 2000*	*Yes*	___
			___	___
			___	___

2-00

Full name of joint inventor (if any) Andreas SASSE

Inventor's signature Andreas Sasse

Citizenship Germany Date of signature 3.10.01

Residence Zur Mühle 13

D-53773 Hennef, GERMANY DEX

Post Office Address SAME AS RESIDENCE